REMARKS

Claims 1, 14-20, 22-32, and 34 are pending in this application.

Applicants have amended claims 1, 14, 15, 17-19, 26-32, and 34. The changes to these claims made herein do not introduce any new matter.

Rejections Under 35 U.S.C. § 103

Applicants respectfully request reconsideration of the rejection of claims 1, 14, 15, 17, 19-22, 25, 27, 30, and 32 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley et al.* ("*Walmsley*") (US 2003/0159036 A1) in view of *Sabin* (US 6,959,091 B1).

The combination of *Walmsley* in view of *Sabin* would not have rendered the subject matter defined in independent claims 1, 27, 30, and 32, as presented herein, obvious to one having ordinary skill in the art. In this respect, Applicants respectfully disagree with the Examiner's assessment given in the Final Office Action on many points. Applicants' detailed analysis is presented in the submission filed on November 30, 2009. Applicants refer to, and reiterate, this detailed analysis. However, it in an attempt to streamline the proceedings, Applicants would like to concentrate in the present submission on the following two arguments:

(1) *Walmsley* does not disclose any integrity check of a private RSA key, and

(2) *Walmsley* does not disclose to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter.

Argument (1): *Walmsley* does not disclose any integrity check of a private RSA key

In the Final Office Action, the Examiner pointed out that Paragraph [0944] of *Walmsley* allegedly discloses an integrity check of a key. Paragraph [0944] of *Walmsley* refers to the keys K_1 and K_2 and the values R and M. *However, none of these keys and values are private RSA keys, as claimed.*

The Examiner further referred to Paragraphs [0486]-[0489], [0652], and [0057]-[0066] as allegedly disclosing a private key K_A that is used in an asymmetric cryptographic method. *However, no integrity check is performed for this private key K_A.*

The private key K_A mentioned in Paragraphs [0486]-[0489] is clearly **different** from the keys K_1 and K_2 mentioned in Paragraph [0944]. Therefore, *Walmsley* may teach an integrity check of the keys K_1 and K_2, and may further teach a private key K_A that is used in an asymmetric cryptographic method, but certainly does not teach any integrity check of a private RSA key, as claimed.

Argument (2): *Walmsley* does not disclose to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter

In the Final Office Action, the Examiner referred to Paragraphs [0657], [0954]-[0957], [0545], and [0601]-[0606] of *Walmsley* as allegedly disclosing the above element. All of these paragraphs have been analyzed in detail in the submission filed on November 30, 2009 (please see pages 10-13 of that submission). In the Final Office Action, the Examiner has not responded to the Applicants' detailed analysis, other than re-listing the above-noted paragraphs. In particular, the Examiner's substantive "Response to Arguments" in the Final Office Action seems to address only the disclosure of an asymmetric cryptographic method in *Walmsley*, and does not refer to the above element of the independent claims at all. Applicants are keen to assist the Examiner in the task of conducting a proper examination, but Applicants can only do so if the Examiner actually responds to the Applicant's detailed analysis.

In the absence of any counter-arguments from the Examiner, *Applicants submit that Walmsley does not disclose to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private*

RSA key parameter, as claimed. In fact, an electronic search revealed that *Walmsley* does not contain any one of the words "corrupt" or "corruption" or "corrupting."

Accordingly, independent claims 1, 27, 30, and 32, as presented herein, are patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin*.

Each of claims 14, 15, 19, 20, 22, and 25 depends from claim 1. Applicants submit that these claims are patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin* for the same reasons set forth above, and because they recite further patentable elements.

Dependent Claims 16-18, 23, 24, 26, 28, 29, 31, and 34

Applicants respectfully request reconsideration of the rejection of claims 16-18, 23, 24, 26, 28, 29, 31, and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Walmsley* in view of *Sabin* and further in view of *Ngo et al.* ("*Ngo*") (US 2003/0097628 A1). Each of claims 16-18, 23, 24, and 26 ultimately depends from independent claim 1. Each of claims 28 and 29 depends from independent claim 27. Claim 31 depends from independent claim 30, and claim 34 depends from independent claim 32. The *Ngo* reference does not cure the above-discussed deficiencies of the *Walmsley* and *Sabin* references relative to the subject matter defined in the present independent claims 1, 27, 30, and 32. Claims 16-18, 23, 24, 26, 28, 29, 31, and 34 are therefore patentable under 35 U.S.C. § 103(a) over the combination of *Walmsley* in view of *Sabin* and further in view of *Ngo* for the same reasons set forth above regarding the applicable independent claim, and because they recite further patentable elements.

Conclusion

In view of the foregoing, Applicants respectfully request reconsideration and reexamination of claims 1, 14-20, 22-32, and 34, as amended herein, and submit that these claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at **(408) 749-6902**. If any additional fees are due in connection with the filing of this paper, then the Commissioner is authorized to charge such fees to Deposit Account No. 50-0805 (Order No. WACHP006).

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, L.L.P.

/Peter B. Martine/

Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 200
Sunnyvale, California 94085
Customer Number 25920